WHITE & CASE

From *Habeas Data* Action to *Omnibus* Data Protection: The Latin American Privacy (R)Evolution

September 2011

"Knowledge will forever govern ignorance; and a people who mean to be their own governors must arm themselves with the power which knowledge gives."[1]

Manuel Martinez-Herrera

White & Case

Latin America: More Privacy than You Would Expect

Whenever you ask a privacy expert about parts of the world with strict data privacy laws, the European Union, with its by now famous EU Data Protection Directive,[2] is unequivocally the first, if not the only region, to come up. If you keep pressing your expert, he/she might start discussing the privacy laws in Asia (the Japanese PIPL and the Hong Kong Personal Data (Privacy) Ordinance being the laws most frequently cited), Canada[3] or Oceania.[4]

However, few experts, if any, will mention Latin America as a "hot" privacy spot. Is this fair? Is it really the case that data protection laws are inexistent or not prevalent in Latin America? Or is this just another misconception?

Let's look at some facts:

- Five Latin American countries—Argentina, Uruguay, Mexico,Peru and Costa Rica—have already enacted comprehensive EU-style data protection laws. This means that approximately 185 million Latin Americans, more or less a third of the total population in the region according to certain rough estimations, are covered by omnibus data protection laws.
- In 2003, Argentina became the fourth country, only after Switzerland, Hungary[5] and Canada, out of a current total of nine to be considered an "adequate protection" jurisdiction by the EU Commission.[6]
- Uruguay, and probably New Zealand as well, are the only countries with real possibilities of being considered "adequate protection" jurisdictions in the near future.[7] If Uruguay achieves this distinction, South America will be, after Europe, the continent with the most "adequate protection" jurisdictions under EU standards.
- Omnibus data protection bills are currently being discussed in, at least, Colombia and Brazil. Chile is also expected to "beef up" its existing law.
- A Habeas Data right exists, in one form or another and with more or less limitations, in most Latin American[8] countries.

For review and comments on drafts of this article, the author thanks Ashley Winton (White & Case, London) and Daniel Clarke (White & Case, London). This article is current as of September 2011.

[1] James Madison, fourth President of the United States (1809-1817).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available* at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[3] Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000.

[4] Australia enacted its Privacy Act in 1988 and New Zealand in 1993.

[5] The EU Commission Decision in favour of Hungary became irrelevant once Hungary joined the European Union in 2004.

[6] This distinction basically means that the EU, potentially the main data privacy "force" in the world, has thoroughly reviewed the country's data

This article was published in a slightly different form in the September 2011 edition of *Latin American Law & Business Report, Vol. 19, No. 9*

From *Habeas Data* Action to *Omnibus* Data Protection: The Latin American Privacy (R)Evolution

The common and easy criticism to this compelling list of facts is that despite the existence of all these data privacy laws and regulations, enforcement is very limited in Latin America and, consequently, almost nobody complies with these allegedly "toothless" privacy regimes. There is, of course, some truth to this argument. A prominent Argentinean data privacy attorney once told this author that he does not know of a single instance in which the Argentinean data protection authority (DPA), the oldest DPA in the region, has issued a sanction against a company for not registering a database or for illegally transferring personal data abroad – both of which are textbook violations under the Argentinean data protection law. Apparently, according to this lawyer, the Argentinean DPA has a limited budget and is more focused on educating than on penalizing.

Nevertheless, it is undeniable that Latin America is awakening, and awakening fast, to the ticking data privacy clock and is unquestionably becoming an important force behind data privacy regulations and one of the main data privacy scenarios to pay attention to.

Habeas Data: How It All Began

Habeas Data is a legal term frequently used but also frequently misconstrued outside Latin America. So then, what is exactly Habeas Data? Its literal translation from Latin would be something like "*that you* [the data subject] *have the data*." This translation is actually an accurate and to-the-point simple explanation of what Habeas Data is: Habeas Data is a right incorporated by many Latin American countries, in most cases in their constitutions and/or in separate laws, by which individuals can request access to any personal data about them held in a database, usually indistinctively of whether it is a public or private database, and, depending on the jurisdictions, also the rectification, update or elimination of the data that can be proven to be incorrect, is no longer true or should remain confidential. This right also encompasses the possibility of filing an action in court if the access, rectification, update or elimination request has not been granted.

It is, therefore, very similar, if not equivalent, to the well known rights to access, rectify, block and/or eliminate personal data included in the EU Directive. In fact, the Habeas Data origins are supposedly European as it was in Germany where the right known as the information self-determination right, the alleged Habeas Data predecessor and not surprisingly another name used in certain Latin American jurisdictions to refer to Habeas Data, was first enunciated. This is the individuals' right to control the information stored and disclosed about them. Such a right is, of course, paramount to protect an individual's image, honor and reputation as it is a way to try to control incorrect/inaccurate information that may damage such image, honor or reputation. Therefore, creating this right makes good sense in countries with civil law legal traditions[9] that value privacy as an important right as such countries, unlike common law jurisdictions, have historically linked privacy rights to the rights to protect one's image, honor and reputation.[10]

The reader might by now be wondering how Habeas Data jumped the pond and made it all the way from Germany to Latin America. In my opinion, there is no clear explanation to this. One important factor might have been that due to certain political/sociological reasons many Latin American countries enacted new constitutions or reformed them during the late eighties and nineties (e.g., Brazil in 1988, Colombia in 1991, Paraguay in 1992, Bolivia in 1995, Ecuador in 1998, Venezuela in 1999, etc.). This was a time when the discussions about privacy rights were starting to gain certain momentum worldwide (the very relevant Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* was issued in 1981 and the EU Directive was passed in 1995) and the Habeas Data right appears to be the constitutional answer of certain Latin American countries to the privacy concerns of their population.

Habeas Data Is Just the First Step

As we have seen, Habeas Data is a right widely spread throughout Latin America. However, this right by itself is far from creating a comprehensive privacy regime capable of fully protecting data subjects' personal data. This argument is reinforced by the fact that Argentina is the only Latin American country currently considered an "adequate protection" jurisdiction by the EU and this consideration was only obtained after its privacy regime evolved from Habeas Data to an omnibus data protection law.

The main limitations of a legal system simply relying on the typical Habeas Data construction are, among others, the following:

- There is no specific governmental supervisory authority (a Data Protection Authority) ensuring compliance, providing support to

privacy regime and has found it satisfactory under its own strict standards. Once a jurisdiction obtains such recognition by the EU Commission, personal data can be sent from the EU to the non-EU anointed country as if sent from one EU country to another (e.g., from the Netherlands to Spain). For more information on the EU "adequate protection" procedure, see Manuel Martinez-Herrera, *Use "Adequate Protection," Avoid I(legally) T(ransmitting) D(ata)*, EuroWatch, Vol. 23, No. 7 (2011).

[7] The Article 29 Working Party issued an affirmative opinion in favour of Uruguay in October 2010. *See* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf. Receiving a positive opinion from the Article 29 Working Party is an essential and imperative step for any jurisdiction that aspires to be considered an "adequate protection" jurisdiction. The Article 29 Working Party is an independent EU advisory body on data protection and privacy formed by the national data protection commissioners of the EU Member States, the European Data Protection Supervisor and a Commission representative. The Commission also provides the Working Party's secretariat.

[8] A Habeas Data right exists, at least on paper, in Argentina, Brazil, Bolivia, Chile, Colombia, Costa Rica, Ecuador, Honduras, Mexico, Paraguay, Peru, Dominican Republic, Uruguay and Venezuela.

[9] All Latin American countries share a civil law tradition inherited from their Spanish and Portuguese colonizers.

individuals in the exercise of their privacy rights or enforcing these rights. It can be argued, however, that this role is performed in the Habeas Data countries by the general judicial system.

- There are no restrictions on transferring personal data to third parties (domestically or abroad).
- Habeas Data does not ensure that the data held in a database is kept in a secure and confidential way.
- Habeas Data does not ensure that personal data collected is only used for the purpose for which it was collected and is kept accurate, updated and no longer than necessary.
- The processing of sensitive data does not receive additional protections.

From *Habeas Data* to EU-Style Data Protection Laws

Argentina was the first Latin American country to realize that Habeas Data was not sufficient by itself and needed to be incorporated into a more robust data privacy regime. Some other Latin American countries, such as Uruguay, Mexico, Peru and Costa Rica have recently followed suit.

It has long been said that one of the main reasons for this Habeas Data-to-omnibus-data protection-law evolution in Latin American countries is to be considered an "adequate protection" jurisdiction by the EU in order to attract more business from Europe. An "adequate protection" jurisdiction might become an appealing place for European companies to open new subsidiaries or branches, outsource operations or use local call or data centers or other type of businesses for which they would usually go to Eastern Europe, India, the Philippines or East Asia, as data can then flow back and forth from that country to the EU as if that country was a Member State.

This is shown, for example, by the preamble to the data privacy bill currently being discussed in Colombia and that is pending review by the Colombian Constitutional Court which clearly states that one of the goals of this bill is for Colombia to be considered an "adequate protection" jurisdiction by the EU.

"Uruguay XXI," the Uruguayan Investment and Export Promotion Institute, also said the following when discussing this topic: *"The EU recognition will open the possibility for major European investments, in particular it will help Uruguay boost its outsourcing industry (call centers, data centers, technology parks) and attract more EU-based companies looking for providers of administrative, financial and other data processing services in Latin America."*[11]

This obviously explains why the Latin American data privacy laws are closely modeled after the EU laws. It is logically easier to obtain a positive finding by the EU Commission if your laws are similar to the EU Data Protection Directive (or to laws that transposed the Directive).

At the Forefront of Latin American Privacy

As mentioned above, five Latin American countries have already enacted omnibus data protection laws.

- **Argentina**: The nation of Maradona and the tango outmaneuvered all other Latin American countries to be the first, and for a good number of years the only, Latin American jurisdiction with a comprehensive data privacy law when it passed the Personal Data Protection Act 25.326 (*Ley 25.326 Protección de los datos personales*) in 2000.

  This law created the first Latin American Data Protection Authority, the National Directorate for Personal Data Protection (*Dirección Nacional de Protección de Datos Personales*). Complementing regulations were issued a year later.

  Thanks to this law Argentina became, and remains to this day, the only Latin American jurisdiction for which the EU Commission has issued a Decision considering that it ensures an adequate level of data protection.

- **Uruguay**: Uruguayans and Argentineans not only share the same accent and their love for football as on the other side of the famous *Río de la Plata* we find the second country in the region to have enacted an omnibus data protection law. Uruguay passed its Personal Data Protection and Habeas Data Action Act 18.331 (*Ley N° 18.331 Protección de Datos Personales y Acción de Habeas Data*) in August 2008. As we can see, Habeas Data remains an important part of the Uruguayan privacy regime to the point that the law incorporates the term in its own name.

  The Uruguayan law is strongly influenced by its Argentinean counterpart. Its regulations were issued in August 2009.

  The Uruguayan DPA is called the Personal Data Controlling and Regulating Unit (*Unidad Reguladora y de Control de Datos Personales*) and is commonly referred to by its acronym, the "URCDP."

[10] For a very interesting discussion about how European societies perceive privacy see James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 403 (2004).

[11] *See* http://www.uruguayxxi.gub.uy/innovaportal/v/1315/2/innova.front/uruguay_recognized_by_the_european_union_as_offering_an_adequate_level_of_data_protection

Thanks to these efforts, as previously explained, the Article 29 Working Party has already vetted Uruguay as a jurisdiction with adequate protection and, consequently, it might be the next country to be anointed by the EU Commission.

- **Mexico**: Mexico was until very recently the last member to join the Latin American privacy club. The Federal Law on Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) was passed on July 5, 2010 and became effective July 6, 2010. Just a year after that Mexico issued draft regulations.

  The Mexican DPA is the Federal Institute for Access to Information and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos*).

- **Peru**: The Personal Data Protection Act 29.733 (*Ley de Protección de Datos Personales*) was one of the last bills signed into law by President Alan García before he was replaced by Peru's new President, Ollanta Humala, on July 28, 2001.

  Only certain articles and parts of the law are now in force. The remaining parts will not enter into force until 30 days after the regulations are issued (which may take several months).

  The Ministry of Justice is in charge of creating Peru's DPA, the Authority for the Protection of Personal Data (*Autoridad de Protección de Datos Personales*), on or before December 16, 2011.

- **Costa Rica:** The Protection of the Individual Against the Processing of his Personal Data Act 8968 (*Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales*) was published in the Costa Rican official gazette on September 5, 2011, and entered into force that same day.

  Prodhab is the acronym for the Agency for the Protection of Individual's Data (*Agencia de Protección de Datos de los habitantes*) which will be Costa Rica's DPA. This agency has to be created within 6 months from the date the law entered into force. Once created, the government will have a maximum of another 6 months to issue the regulations and companies will have a one year grace period to make sure they are compliant with this new law.

A quick look at any of these laws reveals many of the same concepts included in the EU Directive: special treatment of sensitive data; need to notify data subjects or obtain their consent; obligation to keep the data secure; restrictions on transferring data abroad; creation of a data protection authority and a registry of databases; data subjects' right to access, rectify or eliminate their personal data; penalties and sanctions for not complying with the obligations under the laws; etc.

It Is Their Time

Argentina, Uruguay, Mexico and Peru already have robust data privacy laws, as does Costa Rica to a lesser extent; Colombia, Chile and Brazil are discussing how to strengthen their data privacy regimes; the 33rd International Conference of Data Protection and Privacy Commissioners (ICDPPC 2011) will be hosted by the Mexican DPA in Mexico City. These are all obvious signs that Latin America is on the move on the privacy front and that, with the exception of Europe, it can be considered the most active "data privacy region" in the world at this moment.

All these legislative efforts have to be, of course, analyzed with a healthy dose of suspicion due to the enforcement issues we have already commented on and the fact that on multiple occasions privacy bills are discussed for years and years only to get lost within the lawmaking process and the political debate without an actual law being passed (South Africa is a great example of this).

All that being said, the impression is that data privacy is stronger than ever in Latin America and that it will continue to grow in the region with the enactment of new data privacy laws and regulations that will slowly, but inexorably, give rise to more vigilant privacy enforcement by the newly created data protection authorities.

Companies would be wise to start adapting their processing and transfer of personal data in Latin America to the standards required by these laws. The good news is that if these companies are already compliant in Europe they should already be familiar with most of the requirements and obligations under the Latin American data privacy laws.

From *Habeas Data* Action to *Omnibus* Data Protection: The Latin American Privacy (R)Evolution

Manuel Martinez-Herrera *is an International Labor & Employment Law Associate at White & Case LLP, New York. Mr. Martinez-Herrera's practice focuses on counseling multinational employers on cross-border human resources and data privacy issues affecting multiple countries and jurisdictions. Mr. Martinez-Herrera has previous Employment Law experience both in the European Union and in the US. Prior to joining White & Case, Mr. Martinez-Herrera was an associate at one of the major US labor and employment law firms. Before that, Mr. Martinez-Herrera practiced EU and Spanish Employment Law in Barcelona as an associate of the international employment law group of one of the leading Spanish law firms, and corporate law in Buenos Aires at one of the major Argentinean law firms.*

The information in this article is for educational purposes only; it should not be construed as legal advice.